DEPARTMENT OF THE ARMY
HEADQUARTERS, 4th INFANTRY DIVISION
FORT HOOD, TEXAS 76544-5200

AFYB-CG

22 March 2007

MEMORANDUM FOR: 4ID Network Customers

SUBJECT: 4ID, G6 Information Assurance (IA) Policy # 15: Information Assurance Vulnerability Management Enforcement

1. References:

   a. AR-25-1, Army Knowledge Management and Information Technology, 15 July 2005.

   b. AR 25-2, Information Assurance, 14 November 2003.

   c. HQDA CIO/G6 Information Assurance Vulnerability Management Program, Army Information Assurance web page, https://informationassurance.us.army.mil.

   d. Army Policy For The Implementation Of The Information Assurance Vulnerability (IAVA) Process, https://www.acert.1stiocmd.army.mil/policy/Army_IAVA_Policy.txt.

2. Purpose: The Army information assurance vulnerability management program promulgates messages to all system administrators alerting them of vulnerabilities found in automated information systems and software. The messages, titled information assurance vulnerability alerts (IAVA) describe the devices/software affected, prescribe corrective actions to correct or mitigate the vulnerability, and establish suspense for completion of the corrective actions. This policy describes the method of IAVA program enforcement within the 4ID area of responsibility. IAVA messages are promulgated by a list server. Every information assurance officer (IAO), such as system administrators (SA), IA Security Officer (IASO), Information Systems Network Managers (IANM), and IA Manager (IAM) must subscribe to the IAVA list server.

3. Applicability: This policy applies to, and is an AIS / IA operational directive to, all military, civilians, and contractors who plan, deploy, configure, operate, or maintain data communications resources or devices directly or indirectly attached to 4ID networks, regardless of service or agency affiliation.

4. Responsibilities:

   a. 4ID Information Assurance Manager (IAM) will:

      (1) Ensure the Army IAVA program is implemented through out the 4ID area of responsibility.

      (2) Monitor IAVA compliance and reporting

      (3) Direct such actions as are deemed necessary to reduce the risk presented by devices/software found to be non-compliant with current IAVA messages.

      (4) Coordinate activities involving tenants and 4ID.

      (5) Report periodic status to the 4ID G6, 4ID IAM, and others as directed.

   b. 4ID Information Assurance Network Manager (IANM). The 4ID IANM has the following responsibilities:

      (1) Scan the 4ID managed networks for IAVAs that have passed their suspense date.

(1) Scan the 4ID managed networks for IAVAs that have passed their suspense date.

(2) Isolate all devices found to be non-compliant from the network in accordance with this policy.

(3) Re-scan devices reported to be made compliant and return service to those found to be so in accordance with the procedures in this policy.

(4) Report periodic status to the 4ID G6, and others as directed.

c. Information Assurance Security Officer (IASO) will:

(1) Ensure all IT systems and devices are maintained with the most current versions and all IAVA directed remediation is accomplished by the published suspense date.

(2) Ensure that the current IAVA compliance status of all AIS in their area of responsibility is reported in the IAVA compliance reporting database (CRD) for Army organizations and reported to the Installation IAM for non-Army organizations.

d. System Administrator (SA) will:

(1) Understand and monitor the configuration of the IT systems and devices administered.

(2) Maintain all systems and devices with the most current versions of software. Apply remedial actions as directed by IAVAs not later than the published suspense date. Thoroughly test all patches and changes in a non-production environment before applying them to production devices.

5. IAVA Program Enforcement Policy: AIS and devices found to be non-compliant with the Army IAVA program will be isolated from the network as close to the non-compliant device as technically feasible.

a. The IANM will scan the networks for devices non-compliant with IAVAs that have passed their suspense date, or as directed by higher authority.

b. Devices found non-compliant will be immediately isolated from the network as close to the non-compliant device as is technically feasible.

c. If 20 or more devices are found to be non-compliant on a single class C sub-net, the entire network will be isolated and remain isolated until all devices on that sub-net are compliant. In the case where a class C sub-net has been masked and issued to more than one organization, the "20 rule" will be applied to the masked portion of the sub-net. The intent is to prevent a negligent organization from causing an interruption service to an organization that is compliant.

d. The list of non-compliant devices will be provided to the IAM as soon as it is generated, concurrent with the beginning of device isolation actions.

e. The 4ID Information Assurance Office will notify units/sections of the non-compliant devices by the most expeditious means available and provide instructions on how to make the device compliant (provide the IAVA message if they don't have it) and how to get the device returned to service.

f. When the owning organization has remediated the non-compliant device, they must call the 4ID (Help Desk), at 287-0783, and request service be restored to the device.

g. The IANM will re-scan the device and, if verified compliant, will restore it to service, subject to the "20 rule". The "20 rule" states that if the device is on a sub-net that had 20 or more non-compliant devices, service will not be restored until all devices on the sub-net are verified compliant.

6. Non-compliance. Non-compliant devices and systems will be immediately isolated from the network. Army policy is that every device attached to an Army network will be 100% compliant with the Army IAVA program. Mission critical systems that will cause grave harm to mission if removed from service are the very systems that must be patched immediately to ensure their vulnerabilities aren't exploited by hostile forces and random malicious code like viruses and worms. Isolating them from the network minimizes mission impact by protecting them from attacks that can cause the entire system to be torn down and rebuilt, corrupt and destroy data, and deny use of the system for an extended period of time.

7. POC for this policy is the 4ID Information Assurance at DSN 737-0785 or commercial 254-287-0785.

JEFFERY W. HAMMOND
MG, USA
Commanding